TCG PC Client Reference Integrity Manifest Specification

Version 1.4
November 2, 2020
PUBLISHED
Contact: admin@trustedcomputinggroup.org
DISCLAIMERS, NOTICES, AND LICENSE TERMS

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY
WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR
ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use
of information in this specification and to the implementation of this specification, and TCG disclaims all liability for
cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental,
consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any
way out of use or reliance upon this specification or any information herein.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted
herein other than as follows: You may not copy or reproduce the document or distribute it to others without written
permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG
specifications or (b) developing, testing, or promoting information technology standards and best practices, so long
as you distribute the document with these disclaimers, notices, and license terms.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing
through membership agreements.

Any marks and brands contained herein are the property of their respective owners.
CONTENTS

DISCLAIMERS, NOTICES, AND LICENSE TERMS .................................................................................. 1

1 Scope and Context .............................................................................................................................. 3
   1.1 Audience .................................................................................................................................. 3
   1.2 Goals ......................................................................................................................................... 3
   1.3 Relationships to other Documents ......................................................................................... 3
      1.3.1 TCG Documents ............................................................................................................... 3
      1.3.2 Non TCG Documents ....................................................................................................... 4
   1.4 Terms and Definitions .............................................................................................................. 4
   1.5 Keywords ................................................................................................................................. 5
   1.6 Statement Type ........................................................................................................................ 6

2 Background ........................................................................................................................................ 7

3 PC Client Reference Integrity Measurement (PCRIM) ................................................................... 8
   3.1 The PC Client Base RIM .......................................................................................................... 8
      3.1.1 Base RIM Format ............................................................................................................... 8
      3.1.2 RIM Information Model Elements .................................................................................. 9
      3.1.3 Base RIM Signatures ........................................................................................................ 9
      3.1.4 Base RIM signing certificates .......................................................................................... 9
   3.2 PC Client Support RIM ........................................................................................................... 10
      3.2.1 TPM PCR Assertions ....................................................................................................... 10
      3.2.2 TCG Event Log Assertions ............................................................................................. 11
   3.3 EFI System Partition Storage .................................................................................................. 12
      3.3.1 File naming conventions ................................................................................................. 12
      3.3.2 RIM Support File names ................................................................................................ 13

4 RIM Lifecycle .................................................................................................................................... 14
   4.1 RIM Bundle Creation .............................................................................................................. 14
   4.2 Pre Delivery RIM Bundles ...................................................................................................... 14
      4.2.1 Supplemental RIM Bundles ............................................................................................ 14
   4.3 Supply Chain Processing using the RIM ................................................................................. 15
      4.3.1 Optional Reimaging ....................................................................................................... 15
   4.4 Maintenance updates ............................................................................................................... 15
   4.5 Firmware Updates .................................................................................................................. 16

Appendix A: PC Client Base RIM Example ....................................................................................... 17

Appendix E: RIM Guidance for OS developers ............................................................................... 25

Appendix F: References .................................................................................................................... 26
1 Scope and Context

Attester integrity and corresponding attestation evidence are critical to many use cases. DICE [21], TPM [22] and platform specifications [7] were designed to provide information—evidence—helpful for Verifiers to determine the state of a platform—the Attester. To that end the TCG Trusted Attestation Protocol (TAP) Information Model specification [1] was created to outline the information presented by the Attester device to the Verifier. The TCG Reference Integrity Manifest (RIM) Information Model (IM) specification [12] compliments the TAP by providing common information elements used by the Verifier to validate the identity of the RIM’s creator and the integrity of the support files used to provide the integrity reference information.

This PC Client RIM specification complies with the RIM Information Model and provides addition requirements for PC Client platforms that adhere to the TCG PC Client Platform Firmware Profile [7]. This specification describes the RIM file formats, RIM storage locations within the PC Client, and provides references for the content of the RIM support files.

The PC Client RIM is limited to the integrity reference information necessary for TPM Quote validation by a Verifier for measurements taken during the Attester’s boot cycle. Other integrity processes, such as Integrity Measurement Architecture (IMA) [23] are beyond the scope of this specification.

1.1 Audience

This specification is intended to be used by: firmware developers that create firmware compatible with the PC Client Firmware Profile [7]; Verifier developers who need to know the formatting, structure, and usage guidelines for creating and processing a RIM Bundle; and platform developers that need to understand how to create and distribute RIM Bundles. This specification may also be beneficial to OS developers who manage TPM PCRs 8-15.

1.2 Goals

1. To describe the formatting for the common set information elements described by the TCG Reference Integrity Manifest (RIM) Information Model specification
2. To describe the RIM support files for PC Client platforms as required by the RIM Information Model specification.
3. To define default storage locations for RIM Bundles.

1.3 Relationships to other Documents

1.3.1 TCG Documents

There are many TCG documents that use the terminology of Reference Manifest (RM) and Reference Integrity Manifest (RIM). This specification defines the RIM for PC Client platforms.

1.3.1.1 RIM IM

The Reference Integrity Measurement (RIM) Information Model (IM) specification defines an abstract structure for assembling reference measurements (Assertions) that manufacturers and other supply chain entities assert as expected values. The RIM IM requires that a binding specification (this specification) to define a realization of a RIM information model expressions.

1.3.1.2 TAP

The TCG Trusted Attestation Protocol (TAP) Information Model specification provides the information elements used by Verifiers. Not all of the information is required by every Verifier. The RIM is essential for TAP based attestation [1]. The TAP Information Model provides the reference material needed by the Verifier in order to implement the TAP Information Model. Future versions of the TAP Information Model specification may include gathering RIM information from the Attester.
1.3.1.3 FIM
The PC Client Firmware Integrity Measurement (FIM) specification [11] outlines the basic process for collecting, reporting, and processing (attestation) of PC Client firmware.

1.3.1.4 Platform Certificate Profile
The TCG Platform Certificate Profile specification [10] contains assertions about trust made by a platform manufacturer. The certificate asserts the platform’s security properties and configuration as shipped. The Platform Certificate Profile defines a PlatformConfigurationURI attribute that contains “URI where the reference integrity measurements could be obtained by the verifier”. The RIM Information Model specification discusses options for the PlatformConfigurationURI attribute.

1.3.2 Non TCG Documents
1.3.2.1 NISTIR 8060
The National Institute for Standards and Technology Interagency Report (NISTIR) 8060 [3], “Guidelines for the Creation of Interoperable Software Identification (SWID) Tags” is the primary reference for the elements described in this specification. NIST IR 8060 pulls its definitions from ISO-IEC 19770-2 and is accessible on the NIST website. Because this specification is focused on integrity there are further restrictions and additional requirements for the information elements that are above and beyond the guidelines found in NISTIR 8060.

1.3.2.2 ISO-IEC 19770-2 (SWID)

1.3.2.3 XML Signature Syntax and Processing
The XML Signature Syntax and Processing Version 2.0 [8] is an informative W3C Working Group Note that describes XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

1.4 Terms and Definitions

**Asserter:** A supply chain entity, manufacturer, vendor or reseller that produces reference values.

**Assertions:** Reference values.

**Attester:** A platform or platform component that provides evidence to a Verifier as to its state.

**Base RIM:** The Base RIM is a RIM Bundle that provides a verifiable identity of the RIM creator and integrity information of support RIMs. The Base RIM contains a digest of each support RIM. The Base RIM also contains a signature.

**GUID:** Globally Unique IDentifier that is referenced by ISO 19970-2 and is technically identical to the UUID as specified by RFC 4122 [24].

**Reference Integrity Manifest (RIM):** A Reference Integrity Manifest contains structures that a Verifier uses to validate expected values (Assertions) against actual values (Evidence).

**RIM Binding / Binding Specification:** A specification that defines conventions for RIM (and RIM Bundle) formatting, marshalling, serialization, digesting, signing, encryption, realization, location, discovery or storage. And
for describing how the information contained in a RIM Bundle is transmitted between Attesters and Verifiers. For example, a RIM Bundle may be marshalled for conveyance over an IP-based communication protocol or instantiated as a file or collection of files in a file system.

**RIM Bundle**: A collection of a single Base RIM and one or more Support RIMs. A Bundle is created by a single entity at a single point in time.

**RIM Bundle Collection**: A collection of RIM Bundles typically consisting of a Primary RIM Bundle and one or more Supplemental RIM Bundles.

**RIM Creator**: Manufactures, System Integrators, Value Added Resellers, Information Technology (IT) support organizations, or endpoint platform owners that create a RIM instance for an Endpoint platform.

**RIM GUID**: A GUID created as a reference to a specific RIM Bundle. The RIM GUID can be used to link a RIM Bundle to multiple other RIM Bundles.

**Supplemental RIM Bundle**: Additional RIM Bundles added to a RIM Bundle Collection.

**Support RIM**: A support RIM contains assertions about the state or configuration of the device to which the RIM applies (a.k.a., Reference Integrity Measurements).

**SWID**: Software ID tags as defined by ISO-IEC 19770-2.

**SWID Schema**: An XML schema that describes the structure of the SWID tag.

**TCG Event Log**: A log file created by the Core Base of Trust for Measurement (CRTM) that is defined in the TCG PC Client Platform Firmware Profile Specification [7].

**TCG Event Log Expected Values**: A TCG Event Log file, as defined by the PC Client Firmware Profile Specification [7], that is captured by a RIM creator and used as a RIM support file.

**TPM PCR Expected Values**: A TPM PCR structure that is saved to a file captured by the Primary RIM creator and used as a RIM support file (see section 3.2.1).

**Verifier**: A system that analyzes evidence from an Attester to determine the Attester’s state.

### 1.5 Keywords

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document’s normative statements are to be interpreted as described in RFC-2119[2]. Key words for use in RFCs to Indicate Requirement Levels.
1.6 Statement Type

Please note a very important distinction between different sections of text throughout this specification. There are two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, it can be considered a kind of normative statements.

**EXAMPLE: Start of informative comment**

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

**End of informative comment**
2 Background

The TCG TPM 2.0 Provisioning Guidance [6] describes a set of Golden Measurements that “represent the expected default values of the integrity measurements which the boot firmware and subsequent code generates and extends into TPM PCRs”. The Provisioning Guidance document further states that Platform Manufacturers should deliver a list of expected integrity measurements of the platform BIOS, firmware, and other binaries they provide “as shipped”. Golden Measurements should be included in boot firmware updates, in order to support a given device’s lifecycle.

The TCG PC Client Platform Firmware Profile [7] defines a TCG Event Log that captures hashes of firmware and software, firmware configuration settings, and events that are critical to boot operations of the device that extend into the TPM’s Platform Configuration Registers (PCRs). The TCG Event Log can be used by an Attester to serve as the “PCR Log Values” described in the TAP Model that is sent to the Verifier as part of an attestation request. The Verifier needs Reference information in order to validate the log information being sent by the Attester.

The Verifier is also responsible for validating the Quote information sent by the Attester. The Reference information is critical in terms of creating values that can be used to validate the TPM Quote.

A check of the PCR values from a TPM is necessary to ensure that the firmware and firmware configuration has not been altered during post processing and delivery of the Attester device. Once the Attester owner takes possession of the device, they can elect to create RIM bundles to track modifications made to the configuration of the device, if such modifications are required.

End of informative comment
3 PC Client Reference Integrity Measurement (PCRIM)

Start of informative comment

The TCG RIM Information Model specification describes a RIM Bundle that consists of Base RIM and one or more Support RIM (files). The combination of Base and Support RIM represents a RIM Bundle. There may be many RIM Bundles (referred to a RIM Bundle Collection) depending upon the production cycle of a device and the devices associated distribution model.

A RIM Bundle is used by a Verifier as Reference for the appraisal process. To perform the appraisal process, the Verifier also needs an Event Log and a TPM Quote from an Attester (as described by the TAP). The values from the Attester are appraised against the PCRIM during a verification process.

The PCRIM follows guidance as described by the TCG RIM IM (the information model). The following section assumes familiarity with the RIM IM and provides addition requirements for PC Clients.

End of informative comment

3.1 The PC Client Base RIM

Start of informative comment

The Base RIM for PC clients is instantiated as a File. The File contains elements as defined by the RIM IM with the additions or restrictions as noted in this section.

End of informative comment

3.1.1 Base RIM Format

The format for the Base RIM file for PC Clients SHALL be complaint with the ISO/IEC19770-2 (SWID) specification [4] and follow the guidelines presented by NIST IR 8060 (the SWID guidance specification).
3.1.2 RIM Information Model Elements
This specification uses the definitions from Table 1 of the Reference Integrity Information Model specification with the following adjustments:

<table>
<thead>
<tr>
<th>Element</th>
<th>Attribute</th>
<th>Required</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SoftwareIdentity</td>
<td>tagId</td>
<td>Yes</td>
<td>MUST be a GUID that is the same as the ReferenceManifestGuid created for the TCG Event Log’s TCG_Sp800-155-PlatformId_Event field (refer to the TCG PC Client Platform Firmware Profile specification [7] for the definition of the TCG_Sp800-155-PlatformId_Event. The tagID MUST meet the requirements specified by RFC 4122[13])</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
<td>Yes</td>
<td>MUST be set to the BIOS version</td>
</tr>
<tr>
<td>Meta</td>
<td>BindingSpec</td>
<td>Yes</td>
<td>MUST be a String set to “PC Client RIM”. “PC Client RIM” indicates that the RIM Bundle complies with the TCG PC Client RIM Binding specification (this specification)</td>
</tr>
<tr>
<td></td>
<td>BindingSpecVersion</td>
<td>Yes</td>
<td>MUST be in the form of X.Y where X is the major and Y is the minor revision of this specification</td>
</tr>
<tr>
<td>pcURIGLOBAL</td>
<td></td>
<td>Yes</td>
<td>SHALL be a URI equivalent to the URI found in the platformConfigURI attribute within the Attester’s Platform certificate. The platformConfigURI attribute is defined in the TCG Platform Certificate Profile specification [10] and referenced in the TCG Firmware Integrity Measurement [11]</td>
</tr>
<tr>
<td>pcURILocal</td>
<td></td>
<td>Yes</td>
<td>SHOULD be set if the tagCreator stores the RIM bundle on the device</td>
</tr>
<tr>
<td>PayloadType</td>
<td></td>
<td>Yes</td>
<td>SHALL be set to “Indirect”</td>
</tr>
<tr>
<td></td>
<td>supportRIMFormat</td>
<td>Yes</td>
<td>As specified in section 3.2</td>
</tr>
<tr>
<td>Payload</td>
<td>supportRIMURIGlobal</td>
<td>Optional</td>
<td>MAY be set to a URI to retrieve a copy of the Support RIM</td>
</tr>
</tbody>
</table>

Table 1: Changes to the RIM IM information elements

3.1.3 Base RIM Signatures
All RIMs SHALL be digitally signed in compliance with W3C XML Signature Syntax and Processing Version 1.1 [8] with the following requirements:

1. The Base RIM MUST use the Enveloped signature.
   a. The KeyInfoReference element (that provides details on where to get the information to validate the signature) MUST be populated. KeyInfoReference MUST use either KeyName or the X509Data element.
   b. If the KeyName is used then KeyName SHOULD be set to the subjectKeyIdentifier of the signing certificate.
   c. If the X509Data sub element is used to hold a signing certificate then a corresponding Link element MAY exist with a rel attribute set to “signing certificate”. The corresponding href value SHALL be set to “embedded”. Self signed certificates MUST NOT be used in this field.

2. The Base RIM SHALL use a TCG listed algorithm as a hashAlgorithm.
3. The Base RIM SHALL use a TCG listed algorithm as a sigAlgorithm.

3.1.4 Base RIM signing certificates
Start of informative comment
The signer of the Base RIM needs to make the set of Certificates (aka the “Certificate path”) used to validate the Base RIM accessible to Verifiers.

End of informative comment

1. Signing Certificates SHALL use TCG listed algorithms.
2. The Authority Information Access (AIA) extension SHOULD be used to define the location of all of the issuer certificates and the URI of the Online Certificate Status Protocol (OCSP) [20] responder (if supported by the Issuer’s Certificate Authority).
3. The Validity period of the Issuing certificates SHOULD be longer than the expected service life of the device.

3.2 PC Client Support RIM

The Support RIM concept allows for multiple types of support RIM as specified by the supportRIMFormat attribute. This concept enables new formats to be defined in future versions of this specification. The current set of support RIM formats are by no means a comprehensive set of measurements possible for a specific device. Rather they are a snapshot of values as collected within the Event Logs or PCR values taken at the time of the production or modification of the equipment.

There are currently two formats defined for a PC Client support RIM: TPM PCR Assertions and the TCG Event Log Assertions. The supportRIMFormat attribute within the File attribute of the Payload element is used to determine the format being used for the support RIM.

The following section defines the currently defined support RIM formats and how the Support RIM are identified. Support RIM generation is outside the scope of this specification.

End of informative comment

The PC Client RIM Bundle:

1. MUST contain at least 1 Support RIM file.
2. MUST use the supportRIMFormat attribute within the Payload File element within the Base RIM to note the support format(s) being specified.

3.2.1 TPM PCR Assertions

TPM PCR Assertions are optional for those RIM Bundle creators that cannot utilize the Event Log Assertions due to device limitations or other restrictive conditions. TPM PCR Assertions lacks the detail provided by the Event Log Assertion that is useful for diagnostic purposes. When possible, the Event Log Assertion is recommended to be used.

TPM PCR Assertions that are created by the Platform creator should include at least PCRs 0-7 if the Platform Manufacturer does not include an Operating System. The Platform Manufacturer may include other PCRs as appropriate.

TPM PCR Assertions that are created by entities other than the Platform creator (e.g. the Value Added Reseller) should include all PCRs that were changed from the Platform Manufacturer. The VAR may, however, include all PCRs.

One illustrative example is a Platform Manufacturer that installs firmware but not an Operating system. If the Platform Manufacturer is utilizing the TPM PCR Assertion support RIM then only PCRs 0-7 are included in the TPM PCR Assertion. If a Value Added Reseller adds a NIC card that only changes the value for PCR 2, and no other PCR values are affected, then the VAR should create a supplemental RIM Bundle that contains at least the new value for PCR 2. If the VAR installs an Operating System, the PCR 8-15 should be included as well.

End of informative comment

1. If the TPM PCR Assertions is used then the supportRIMFormat attribute within the Base RIM SHALL be set to "TPM_PCR_Assertions".
2. TPM PCR Assertions MUST utilize the data from the output of the TPM2_PCR_Read command as defined in the Trusted Platform Module Library Part 3 [19]. The data is equivalent to TPM 2.0 PCR Values defined in the TCG Trusted Attestation Protocol (TAP) Information Model specification. According to the Trusted Platform Module Library Part 3 this information contains:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UINT32</td>
<td>pcrUpdateCounter</td>
<td>The current value of the PCR update counter</td>
</tr>
<tr>
<td>TPML_PCR_SELECTION</td>
<td>pcrSelectionOut</td>
<td>The PCR in the returned list</td>
</tr>
<tr>
<td>TPML_DIGEST</td>
<td>pcrValues</td>
<td>The contents of the PCR indicated in pcrSelect as tagged digests</td>
</tr>
</tbody>
</table>

Table 2: TPM2_PCR_Read command output

3. The TPM PCR Assertion for a primary RIM Bundle MUST contain (at a minimum) values for the first seven PCRs (PCR 0-7). As an example, a Platform Manufacturer that does not install an Operating System would create a Supplement RIM of type TPM PCR Assertion that includes only PCRs 0-7.

4. The TPM PCR Assertions MUST include all supported TPM hash algorithms supported by the platform firmware and the TPM.

The System Integrator, or Value Added Reseller that adds an OS should create a RIM Bundles that include new support RIM covering PCRs 8-15 at a minimum.

3.2.2 TCG Event Log Assertions

The TCG Event Log Assertions uses a supportRimFormat attribute set to "TCG_EventLog_Assertion".

The TCG Event Log Assertion Support RIM is a binary file (no formatting) containing the Events captured by the S-CRTM as specified by the PC Client Platform Firmware Profile [7]. An example of the event log can be found in Appendix A: PC Client Base RIM Example.
3.3 EFI System Partition Storage

**Start of informative comment**

Storage for the PC Client RIM Bundles is defined in this section as convenience for the end user. OEMs, System Integrator, and Value Added Resellers should use the platformConfigURI attribute within the Platform Certificate in order to provide a flexible, agile, and security centered approach for Verifiers to obtain RIM Bundles.

**End of informative comment**

The Primary RIM Creator (the entity that creates the initial RIM Bundle) SHALL place the RIM Bundle on the Attester device within a tcg/manifest directory located on the EFI System Partition (ESP). Per the SWID guidance document [3] a subdirectory named “swidtag” is used to hold the Base RIM file. Another subdirectory of the tcg directory named “rim” holds the RIM support files. The directories used by a PC Client for storing RIM files SHALL be:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>/boot/tcg/manifest/swidtag</td>
<td>Base RIM Files</td>
</tr>
<tr>
<td>/boot/tcg/manifest/rim</td>
<td>Support RIM Files</td>
</tr>
</tbody>
</table>

*Table 3: Directory Structure for RIM Files*

### 3.3.1 File naming conventions

**Start of informative comment**

Since there can be multiple organizations creating RIM Bundles for a given device a naming convention is required ensure the uniqueness of each RIM file.

**End of informative comment**

#### 3.3.1.1 The Base RIM file name

Per the NISTIR 8060 SWID guidance document [3] the following naming convention SHALL be used:

For the Base RIM file:

```
<name of the tag creator> + <product name> + <RIM version>.swidtag
```

Where:

1. “name of the tag creator” is the “name” attribute of the Entity element defined in the RIM Information Model specification
2. “product name” is the “name” attribute of the SoftwareIdentity element defined in the RIM Information Model specification.
3. “RIM version” is the “version” attribute of the SoftwareIdentity element defined in the RIM Information Model specification. Note that version attribute is set to BIOS version as specified in section 3.1.2.

Example: acme.com.BigProduct.3.swidtag
3.3.2 RIM Support File names
The TCG Event Log Assertions files SHALL use the following naming convention:

<name of the tag creator> + <product name> + <product version>.rimel

The TPM PCR Assertions files SHALL use the following naming convention:

<name of the tag creator> + <product name> + <product version>.rimpcr

Examples:

acme.com.BigProduct.3.rimel
acme.com. BigProduct.3.rimpcr
4  RIM Lifecycle

Start of informative comment

The RIM Information Model specification describes a lifecycle that allows for multiple organizations to participate in the production, distribution, and maintenance of the Attester Device. For PC Clients the RIM Bundle is inherently bound to the Firmware lifecycle. The RIM Bundle should be updated during the process of updating the Firmware.

End of informative comment

4.1  RIM Bundle Creation

Start of informative comment

The Primary RIM Bundle is installed by the Platform Supplier (the tagCreator). The RIM Bundle is installed in the EFI partition in accordance with section 3.3.

End of informative comment

4.2  Pre Delivery RIM Bundles

Start of informative comment

When a System Integrator or Value Added Reseller make modifications that require a new RIM Bundle, the RIM Bundle is installed in the EFI partition in accordance with section 3.3 Error! Reference source not found. The RIM Bundle is considered “supplemental” to the Primary RIM Bundle created by the Attester Device Manufacturer.

End of informative comment

4.2.1  Supplemental RIM Bundles

Start of informative comment

The RIM Information Model specification allows for pre-delivery modifications by System Integrator and Value Added Resellers as well as post-delivery modifications by IT organizations. A modification will require the creation of a supplemental RIM Bundle if the modification changes any reference value contained within the existing RIM Bundle collection. Examples of modifications that require a new RIM Bundle will include:

- Firmware updates that occurred after the device has completed the production cycle.
- Modification of a system component that contains Option ROMs (e.g. NIC or Graphic cards).
- Installation of an Operating System.
- Installation of an EFI user application (e.g. system diagnostic applications).
- Modification of the firmware configuration that may change measured settings (e.g. boot order, secure boot enable, etc.).

As discussed in the RIM information Model specification, the VAR sets the VAR specific information in the entity element of the Base RIM. The VAR also needs to provide either a TCG Event Log Assertions or a TPM PCR Assertions File(s) along with payload file hashes placed in the Base RIM file. Each VAR should only create a single RIM Bundle.

End of informative comment

The System integrator or Value Added Reseller can make a supplemental RIM Bundle that provides a new set of RIM files as illustrated in figure 2:
1. Supplemental RIM bundles SHALL have the supplemental attribute within the Base RIMs SoftwareIdentity element be set to “true”.

2. The Rim Bundle file names are unique and should not conflict with the Primary RIM Bundle. The System Integrator or Value Added Reseller SHALL NOT remove any RIM Bundle as the information in the other RIM Bundles may provide valuable information in an investigation attempting to track down unauthorized modification detected by a Verifier.

As an example, the following illustrates a Linux based directory structure after the example in this section is completed:

```
/boot/tcg/manifest/
    |-- rim/
    |   |-- Acme.com.BigProduct.1.rimel
    |   |-- Acme.com.BigProduct.1.rimpcr
    |   |-- Example.com.BigProduct.1.rimel
    |   |-- Example.com.BigProduct.1.rimpcr
    |-- swidtag/
    |   |-- Acme.com.BigProduct.1.swidtag
    |   |-- Example.com.BigProduct.1.swidtag
```

### 4.3 Supply Chain Processing using the RIM

**Start of informative comment**

An organization procuring a new device (an Attester Device owner or designated Maintenance Organization) that applies this specification may choose to use the RIM as a means of verifying the Firmware and Boot Manager installed on the device. This process involves the use of a Verifier to perform either the PCR Composite or Event Log Verification. Part of the process involves the transfer of all RIMs on the device to the Verifier. The Verifier is responsible for obtaining the Trust Anchors/Certificate paths used for validating the signatures on the RIMs prior to performing the validation.

**End of informative comment**

#### 4.3.1 Optional Reimaging

**Start of informative comment**

Some organizations may choose to reimage the device for security or maintenance reasons. This generally involves using an OS specific installer that will remove any existing OS and install an approved OS (not necessarily the newest available version) as well as performing some initial configuration and setup the device needs to meet local organizational policies and guidelines. This may invalidate some or all of the RIM Bundle Collection(s). The re-imaging may also (optionally) include reflashing the firmware to a known revision. If the organization chooses to perform PCR Composite Event Log Verification after re-imaging then the guidance for this case is:

1. Back up the RIM delivered with the device as it may be destroyed when the device is re-imaged.
2. Create a new RIM when the device is re-imaged. This includes signing the RIM with a signing key that has an Organization-approved Certificate.
3. Verify that the new RIM Bundle contains correct measurements for each device using an OEM provided, commercially available, or open source tool (if available). These tools may require the RIM Bundle as a prerequisite or require internet access to obtain RIM Bundles associated with the newly installed OS and or firmware.
4. Import the new RIMs into the Verifier for future verifications.

**End of informative comment**

### 4.4 Maintenance updates

**Start of informative comment**
As described in the RIM Information Model, an IT Organization (an Attester Device owner or designated Maintenance Organization) may decide to manage configuration changes by creating RIM Bundles. The new RIM Bundle is considered a supplemental RIM and follows section 4.2.1. Refer to the Maintenance update section (section 5.3) of the TCG Reference Integrity Manifest (RIM) Information Model specification for further details.

End of informative comment

4.5 Firmware Updates

Start of informative comment

Firmware updates require an updated RIM to be created by the Platform Manufacturer (or delegated representative). The updated RIM should follow the guidance given in the TCG Reference Integrity Manifest (RIM) Information Model specification section 5.4.

End of informative comment
Appendix A: PC Client Base RIM Example

The following example uses an 2048 bit RSA key pair with an associated Self signed certificate representing the Example.com corporation. The following parameters will be used:

Software Identity Name: Example.com BIOS
version : 01
tagId: 94f6b457-9ac9-4d35-9b3f-78804173b65as
tagVersion:0
Entity (tagCreator) Name
Regid: http://Example.com
Role: softwareCreator tagCreator
Links:
installation media url: https://Example.com/support/ProductA/firmware/installfiles
Meta:
colloquialVersion: Firmware_2019
Edition: 12
Product: ProductA
Revision: r2
PayloadType: Indirect
PlatformManufacturerStr: Example.com
PlatformManufacturerId: 00201234
PlatformModel: ProductA
PlatformVersion:01
FirmwareManufacturerStr: BIOSVendorA
FirmwareManufacturerId: 00213022
FirmwareModel:A0
FirmwareVersion: 12
BindingSpec: PC Client RIM
BindingSpecVersion: 1.2
Payload:
Directory: /boot/tcg/manifest/swidtag
File1: Example.com.iotBase.bin
Version: 01.00
size= 15400
Key used for the example:

An RSA 2048 bit key will be used as the key for signing the Base RIM. Keys and certificate will be shown in PEM format. The TCG Log will be show in base 64 encoding.

Private Key (RSA 2048 bit private key – no password):

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAp3WVYaRJG7EABjbAdqDYZXFSTV1nHY9Ol9A5+W8t5xwBXBryZCGWxERG5rKWypx+dqzj+cFpxxkM6N18jEhQ1x/CEZePEJqpluBO5w2wTEO7hqtMatqgDDMeDRxUulpP8LGP00vh1wyDFFew90d9tvbT3bcLvFh3a3ap9bTm6aBqPup5CxprzwiU2wZfgkDytYBVm+8bhKkMaUrgpNyM+5BAg2zl/Fgw0qotjaGr7PzbH+urCvAgbKLMPoWkVLgAE8Qw98HTf0YSFHCh7VYQySrzlinaOBFSgviR72kHemH2IWjDQeHryVLOpikjVVLipjWe6zzze22S66Q/LmjQIDAQABAoIBAHjxv6J6XfVNMeXzE

DHLaGdJ2j3cB7xf4As5CzQPvETNW2YQOGcwwOqpKLNqFvqacl45+1qlLcbBT3Z_U+ZNgFLFa7kdEeCCsr2B0BuUrRLxxr1IEZsCXSZ0oPlUmKhfCf+drWjVAvujiCPH4IImkA3fMNk8heDqg8s8vRixZX35BmGQnmn91EhVHY/0uzVasZ7wHxDORapChoZKMu8AUYDunjib6E6vCzlj4qaJ8MB7Q1uNPWUrW65NX9rM7Lfl1LxVFGPQXQ33qD5

dlEjctg3iec5TEBvDla9r+Yb5I/Uz1xVOBZuBM2dYf+THHVqD+12Aj+xdjamiDFlu

FAUDQCEcIGeYEA3bIMoRIrL0RthRU00YWRtEZE/NAXx1YU99jGo3SdtOIsQZkLBaG9+H4k4p69MAFzYgX1uxK7ARNm0pBavKwjIPBvIoUKB/MdHL7hEXiXE6VpN0vb

nFRIIUhFwCMFq5WGS032HeRqgZDxKmCaODLTsqnh5IrR9ZsssJPAUCgYEawsf

eZbs6kdGV5e/EELeZiG4znRy42Nt2cqlBfrW4qy/1md90wkyJh9xUtXLxQa0juzp

erTopmOftVzOFOpCw249CIJji70KySZIFX/K92ypbVVG1gi34K+Mnse3ZrR0R/Pc

1ypxNEQtjAovZCTAddshN6VsZPj7s87UHd2ukCgYATSXdoPXXjxjTNXizcrvXJUYc0d04Q2pjI+EdoFMROuDFdEdwnqLyMr7enqY9smIP8ALO9QPq4X1wpoo014/
yC152flv4DMh4pjXuNm6BtitXISYWYNuuzgEtxB5Q/HJHg7Ox65kd4Hcsp1l9Z

mfmRyiCGBkTxcaUEUg3QKQbQCNGWYCtKbj/kbCrz64FpbquNscFJe1yi2/Hba

ilOZ6hj+xPIlNkyT/WO1A1qweV2rlIGYvNtUfE7N6PwyrrpHIBsSICYz+H+clfC

OC9ckcWgRqDhY6qz/0AY8TLV+/DgANy1OpiUMgZt5clQMP7ika1/QxNCWgtnEN

lb1ZIQKbGQDAB/6E/NeR8NNO+FT5pDlMB9y10ybmAW6tEZoGtuYzd6MPC6xhHUILYO

xf2n9yOSISBei4nOsA87eZEX2rsli+/IoRKp3/Orw68s6crQzMYy1jkGbrAqnlh2/p7LL73xh/srRHCFRmCP+5RSwef/4T+a1Pd2aGCGOFbiammHJDEVA==

-----END RSA PRIVATE KEY-----
X509 Certificate holding the public portion of signing key used for validating the signature of the RIM:

-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAgIBAgJr6VBbBm5MA0GCsGqSGSlb3DQECBWcUAMFMxMzCAJBgNV
BAYTA1VTMQswCQYDVQQIJDWQTEQMA4GA1UECgwHRXhhBxBsZTERMA8GA1UECwI
UENDbGlbnQxExJAgBqNVBABMCCVUY4WiwbGVDQTAeFw0yMDAyMTA5NzIzMDdaFw0y
OTEyMTkzNzI2M0MwFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAy
MTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5
NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIz
MDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDda
MFA0GCSqGSIb3DQEBCwUA4IBAQBl2Bu9xpnHCEeebja1+ILQBXJxd6q5+9xqU3sPz
KQxszsZuk7QcSvVd/1v8mquw0PwbF0KrmhflPWP+iouwiNqpG5PhYxhpH9t0sOfib
NLOXhmudt9YoqEYq+MHOLXyn9stX8gkgtfVBDrutuMKyOTf46a68TUCgbR2rnyz
O/656sq54CPDQLyQWRBM+4gN8e00UWTkpBI6/1EUBwkJA6WdlKKe8umVxUPWYYHTZ
70QqNrynln36ycAnZABDzEaj4tMzBjAfUsfesty6Ggxx1WbyZL6YzXYALwYaYvr
crTlEynFynKxuCfDnr1SAHDMS65BY
-----END CERTIFICATE-----

X509 Example.com CA Certificate used to validate the Certificate Path of the Certificate:

-----BEGIN CERTIFICATE-----
MIIDjDCCAnSggAWiBAgIjJALeA1Q472tZoMA0GCsGqSGSlb3DQECBWcUAMFMxMzCAJBG
NvBAyTA1VTMQswCQYDVQQIJDWQTEQMA4GA1UECgwHRXhhBxBsZTERMA8GA1UECwI
UENDbGlbnQxExJAgBqNVBABMCCVUY4WiwbGVDQTAeFw0yMDAyMTA5NzIzMDdaFw0y
OTEyMTkzNzI2M0MwFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAy
MTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5
NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIz
MDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDdaFw0yMDAyMTA5NzIzMDda
MFA0GCSqGSIb3DQEBCwUA4IBAQBl2Bu9xpnHCEeebja1+ILQBXJxd6q5+9xqU3sPz
KQxszsZuk7QcSvVd/1v8mquw0PwbF0KrmhflPWP+iouwiNqpG5PhYxhpH9t0sOfib
NLOXhmudt9YoqEYq+MHOLXyn9stX8gkgtfVBDrutuMKyOTf46a68TUCgbR2rnyz
O/656sq54CPDQLyQWRBM+4gN8e00UWTkpBI6/1EUBwkJA6WdlKKe8umVxUPWYYHTZ
70QqNrynln36ycAnZABDzEaj4tMzBjAfUsfesty6Ggxx1WbyZL6YzXYALwYaYvr
crTlEynFynKxuCfDnr1SAHDMS65BY
-----END CERTIFICATE-----

TCG Event Log used as a Support RIM (Base64 encoded):
PC Client RIM:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<SoftwareIdentity xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd" xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" corpus="false" name="Example.com BIOS" patch="false" supplemental="false" tagId="94f6b457-9ac9-4d35-9b3f-78804173b65as" tagVersion="0" version="01" versionScheme="multipartnumeric" xml:lang="en">
  <Entity name="Example Inc" regid="http://Example.com" role="softwareCreator tagCreator"/>
  <Link href="https://Example.com/support/ProductA/firmware/installfiles" rel="installationmedia"/>
  <Payload>
    <Directory name="rim">
      <File xmlns:SHA256="http://www.w3.org/2001/04/xmlenc#sha256" SHA256:hash="4479ca722623f6c47b703996ced3c081b06b1a8e8a897db70137b07c546848" name="Example.com.iotBase.bin" size="7549"/>
    </Directory>
  </Payload>
  <Signature xmlns="http://www.w3.org/2000/09/xmlsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlsig-more#rsa-sha256"/>
      <Reference URI=""/>
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmlsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>fze9UG1Ft9l80Yn8Z4oDTy7G0iCtk+y7hloOru6pDi=</DigestValue>
    </SignedInfo>
    <SignatureValue>b21c8nvkjYO0MZvm8quOILkd/ocTrdpQ555G7mKELy4wDHRxKe3LLdKXOFpb9A9oTwtdEXZhTCahwdt31YALmuTSY4kBORuPDsaby/Cte/35/2gGwkZEE1DNBVXAG97SiuBd5koebcT8TtdGGis6wrUzcDnFXEt3LLAU8ZHhl7weqeyuqzNP12teCpb2Ru9FDWBOUjgOeBo7P6qdJJCG3txmsD1pjA92zgzuLzwY1B+sPk8ac5n9lXOgaard2MUiijmKrGjzOYEltgMQ+a5ncyZtb8HhdC93xnk0IllaG5wuv1Ribeg/Zr6z5k4Yg6Z+ErOPqlDSyPJMZEJZdkQ==</SignatureValue>
    <KeyInfo>
      <KeyName>2fdeb8e7d030a2209daa01861a964fedecf2bcc</KeyName>
      <KeyValue/>
      <RSAKeyValue/>
    </KeyInfo>
  </Signature>
</SoftwareIdentity>
```

Appendix E: RIM Guidance for OS developers

Operating systems that manage the TPM’s PCRs 8-15 need to provide RIM Bundles during OS installation and updates to those PCR values that change when OS updates are distributed. RIM Bundle distribution can be accommodated by the OS packaging or installation/update services by including a RIM Bundle to be installed on the EFI partition.

An Operating system that manages the TPM’s PCRs 8-15 should provide PC Client RIM Bundles and include the instance in any OS installation or update process that effects any of the PCR values. This is potentially operationally infeasible, depending on how the OS loads and measures drivers (in parallel).

The OS RIM should follow the requirements for Supplemental RIMs as defined in section 4.2.1.

The Event Log Assertions file should exclude any PCR’s not measured into by the OS.

For the TPM PCR Log Assertions the TPML_PCR_SELECTION (as defined in the Trusted Platform Module Library Part 3 [19]) should be set to contain only PCRs 8-15 that are applicable to the OS.

Most operating systems provide package management subsystems that utilize publicly accessible mirrors to assist in the installation and update processes. These systems should provide RIM Bundles that are specific to the device configuration.

Any packaging of Firmware updates (e.g. rpm, deb, msi, etc.) should include the associated RIM Bundle. Any installation/update of OS packages that include firmware updates should include placement of the RIM Bundle in accordance with the EFI System Partition Storage section. The definition of the packaging is out of scope for this specification.
Appendix F: References


[17] NIST, The SWID Tag Validation (SWIDVal) Tool Version 0.5.0, https://csrc.nist.gov/CSRC/media/Projects/Software-Identification-SWID/tools/swidval-0.5.0-swidval.zip


[21] FOUNDATIONAL TRUST FOR IOT AND RESOURCE CONSTRAINED DEVICES
https://trustedcomputinggroup.org/work-groups/dice-architectures/

